CLAIMS

What is claimed is:

Sub a1

1. A method comprising:

storing a current sort encryption key (SEK) at a first destination in an internal memory of an electronic component;

storing a next SEK at the first destination in the internal memory;

providing the electronic component to a second destination; and

recovering a private key at the second destination from a key bundle based on the current SEK, the next SEK and a plurality of bundles received at the second destination.

2. The method of claim 1, wherein prior to storing the current SEK at the first destination, the method further comprises:

transferring at least a first bundle to the first destination via a first link; and

transferring at least a second bundle to the first destination via a first out-of-band information carrying mechanism.

3. The method of claim 2, wherein the first bundle includes a plurality of configuration window (CWIN) bundles.

4. The method of claim 3, wherein each of the CWIN bundles includes a configuration window material, the configuration window includes (i) a first key identifier associated with the current SEK, (ii) the current SEK, (iii) a second key identifier associated with the next SEK, (iv) the next SEK and (v) a group integrity check value for a first encryption key and a second encryption key.

5. The method of claim 4, wherein the configuration window material is encrypted with the first encryption key and the second encryption key.

6. The method of claim 5, wherein each CWIN bundle further includes a group identifier associated with the first encryption key and the second encryption key.

7. The method of claim 3, wherein the second bundle includes a plurality of sort encryption key (SEK) bundles.

8. The method of claim 7, wherein each of the SEK bundles includes (i) a sort encryption key, (ii) a key identifier associated with the sort encryption key and (iii) an integrity check value associated with the sort encryption key.

9. The method of claim 2, wherein prior to storing the current SEK at the first destination, the method further comprises:

transferring the plurality of bundles to the second destination, the plurality of bundles includes a third bundle and a fourth bundle.

10. The method of claim 9, wherein the third bundle is transferred to the second destination via a second link.

11. The method of claim 9, wherein the fourth bundle is transferred to the second destination via a second out-of-band information carrying medium.

12. The method of claim 9, wherein the third bundle is a plurality of second part bundle encryption key (BEK_{p2}) bundles, each of the BEK_{p2} bundles includes a second part of the bundle encryption key and a combined integrity check value associated with a first encryption key and a second encryption key.

13. The method of claim 12, wherein the second part of the bundle encryption key and the combined integrity check value are encrypted with the first encryption key and the second encryption key.

14. The method of claim 12, wherein each BEK_{P2} bundle further includes a group identifier associated with the first encryption key and the second encryption key.

15 The method of claim 9, wherein the fourth bundle includes a plurality of configuration encryption key (CEK) bundles.

16. The method of claim 15, wherein each of the CEK bundles includes (i) a configuration encryption key, (ii) a key identifier associated with the configuration encryption key and (iii) an integrity check value associated with the configuration encryption key.

17. A method comprising:

at a first destination, recovering a current sort encryption key (SEK) and a next SEK based on information within a first plurality of incoming bundles and storing the current SEK and the next SEK in an internal memory of an electronic component; and

at a second destination, upon receipt of the electronic component, recovering a private key from a key bundle based on the current SEK, the next SEK and a second plurality of incoming bundles.

18. The method of claim 17, wherein the current SEK represents a current period of validity for configuration of the electronic component.

19. The method of claim 17, wherein the next SEK represents a next period of validity for configuration of the electronic component.

20. The method of claim 19, wherein the private key is prevented from being recovered if the next period of validity has lapsed.

21. The method of claim 17, wherein the first plurality of incoming bundles includes a plurality of configuration window (CWIN) bundles.

22. The method of claim 21, wherein each of the CWIN bundles includes (i) a first key identifier associated with the current SEK, (ii) the current SEK, (iii) a second key identifier associated with the next SEK, (iv) the next SEK

and (v) a group integrity check value for a first encryption key and a second encryption key.

23. The method of claim 22, wherein the first key identifier, the current SEK, the second key identifier, the next SEK and the group integrity check value are encrypted with the first encryption key and the second encryption key.

24. The method of claim 23, wherein each CWIN bundle further includes a group identifier associated with the first encryption key and the second encryption key.

25. The method of claim 17, wherein the first plurality of incoming bundles includes a plurality of sort encryption key (SEK) bundles.

26. The method of claim 25, wherein each of the SEK bundles includes (i) a sort encryption key, (ii) a key identifier associated with the sort encryption key, (iii) an integrity check value associated with the sort encryption key.

27. The method of claim 17, wherein the second plurality of bundles includes a plurality of first part bundle encryption key (BEK_{p2}) bundles and a plurality of second part bundle encryption key (BEK_{P2}) bundles.

28. The method of claim 27, wherein each of the BEK_{P2} bundles includes a second part of the bundle encryption key and a group integrity check value for a first encryption key and a second encryption key.

29. The method of claim 28, wherein one of the BEK_{p2} bundles includes a first part of the bundle encryption key and an integrity check value associated with the current SEK.

30. The method of claim 29, wherein one of the BEK_{p2} bundles includes a first part of the bundle encryption key and an integrity check value associated with the next SEK.

31. The method of claim 30, wherein the bundle encryption key is recovered upon recovering the first and second parts of the bundle encryption key.

32. The method of claim 31, wherein the private key is recovered using the bundle encryption key.

33. A method comprising:

receiving at least a first bundle via a first link;

receiving at least a second bundle via a first out-of-band information carrying mechanism;

recovering a current sort encryption key (SEK) and a next SEK based on information contained in the first bundle and the second bundle; and

storing the current SEK and the next SEK in an internal memory of an electronic component.

34. The method of claim 33, further comprising transferring the electronic component to a second destination.

35. The method of claim 34 further comprising receiving at least a third bundle via a second link;

receiving at least a fourth bundle via a second out-of-band information carrying medium;

recovering based on information in the third bundle, fourth bundle, the current SEK and the next SEK.

36. The method of claim 35 further comprising recovering a private key based on the bundle encryption key.

37. A network comprising:

a source to output a first collection of encrypted keying material and a second collection of encrypted keying material;

a first destination to receive the first collection of encrypted keying material, to decrypt keying material originating from the first collection of encrypted keying material for recovery of sort encryption keying material and to store the sort encryption keying material into an internal memory of an electronic component; and

a second destination to receive the second collection of encrypted keying material, to decrypt keying material originating from the second collection of encrypted keying material for recovery of at least private key for subsequent loading in the internal memory.

38. The network of claim 37, wherein the first destination is physically separated from the second destination.

39. The network of claim 37, wherein the sort encryption keying material includes a current sort encryption key (SEK) and a next SEK.

40. The network of claim 39, wherein the current SEK and the next SEK collectively represents a period of validity in which the electronic component must be configured.

41. The network of claim 37, wherein the second destination further recovers a digital certificate chain from the second collection of keying material and loads the digital certificate chain into the internal memory.